JOINT FORCE HEADQUARTERS WISCONSIN
WISCONSIN NATIONAL GUARD
2400 WRIGHT STREET
POST OFFICE BOX 8111
MADISON WISCONSIN 53708-8111

AIR NATIONAL GUARD ACTIVE GUARD RESERVE (AGR)
VACANCY ANNOUNCEMENT (MVA) NUMBER 19-83

OPENING DATE: 22 February 2019

CLOSING DATE: 22 March 2019

UNIT/LOCATION: CRTC, Volk Field, WI

POSITION: Cyber Surety

MILITARY AFSC REQUIREMENTS: 3DX5X

MINIMUM SKILL LEVEL REQUIRED: 5

AREA OF CONSIDERATION: Open to all eligible to enter WI ANG AGR Program
Must possess 3DXXX series AFSC w/ a 5-level
No Trainees Accepted.

FILL DATE: TBD

SALARY RANGE: Pay and allowance commensurate with military pay.

MINIMUM GRADE REQUIRED: SrA/E-4

MAXIMUM GRADE AUTHORIZED: MSgt/E-7

MAXIMUM GRADE AVAILABLE: MSgt/E-7

MINIMUM QUALIFICATION REQUIREMENTS

1. Member must be medically qualified IAW AFI 48-123, Medical Examination and Standards. Applicants cannot be subject to any flagging action for medical purposes. ANG members entering on full-time duty must have a current physical examination (within 36 months) prior to entry date. Individuals transferring from title 10 USC (active duty or statutory tour) are not required to have a new physical unless the previous physical is over five years old at the time of entry onto AGR status. Selected individual must have an HIV test completed within 6 months of AGR start date.

2. Members must meet physical fitness standards IAW AFI 36-2905, Air Force Fitness Program.

3. Applicants with family members currently on-board are cautioned to review ANGI 36-101 for assignment restrictions.

4. Personnel must have sufficient retainability to permit completion of tour of duty. Cannot be eligible for or receiving an immediate Federal (Military or Civilian) retirement annuity.

5. **Each application will be screened for all mandatory AFSC entry criteria, if degree requirements are required, please enclose copies of transcripts.**

6. **While there is no minimum time in position required for application, if selected individual has less than 18 months in current position on initial tour or 12 months in position on subsequent tour, final approval is contingent upon TAG waiver.**

7. At a minimum, applicants must be able to obtain and /or maintain a favorable adjudicated personnel security investigation that is commensurate with their currently assigned AFSC. Inability to maintain a favorable background investigation or required security clearance may result in administrative action, including termination from employment.

CONDITIONS OF EMPLOYMENT

1. Individuals selected will be ordered to/or continued on full-time military duty under the provisions of Title 32 USC 502(f). Subsequent tours are at the discretion of the State Adjutant General. Member must remain in initially assigned position for a minimum of twelve months.

2. Individuals selected for AGR tours that cannot attain 20 years of active federal service prior to reaching mandatory separation, must complete a Statement of Understanding in accordance with Attachment 2 of ANGI 36-101.

3. Applicants participating in the ANG Incentive Program may be terminated upon entry into full-time National Guard duty. See specific incentive agreement for termination rules.

4. Applicants must not have been separated "for cause" from active duty or a previous AGR tour.

5. Existing ANG Promotion Policies apply.

BRIEF DESCRIPTION OF DUTIES:

Performs risk management framework security determinations of fixed, deployed and mobile information systems (IS) and telecommunications resources to monitor, evaluate and maintain systems, policy and procedures to protect clients, networks, data/voice systems and databases from unauthorized activity. Identifies potential threats and manages resolution of communications security incidents. Enforces national, DoD and Air Force security policies and directives to ensure Confidentiality, Integrity and Availability (CIA) of IS resources. Administers and manages the overall cybersecurity program to include Emissions Security (EMSEC) and Computer Security (COMPUSEC) programs. Conducts cybersecurity risk management framework assessments; ensures enterprise cybersecurity policies fully support all legal and regulatory requirements and ensures cybersecurity policies are applied in new and existing IS resources. Identifies cybersecurity weaknesses and provides recommendations for improvement. Monitors enterprise cybersecurity policy compliance and provides recommendations for effective implementation of IS security controls. Evaluates and assists IS risk management activities. Makes periodic evaluation and assistance visits, notes discrepancies, and recommends corrective actions. Audits and enforces the compliance of cybersecurity procedures and investigates security-related incidents, classified message incidents, classified file incidents, classified data spillage, unauthorized device connections, and unauthorized network access. Develops and manages the cybersecurity program and monitors emerging security technologies and industry best practices while providing guidance to unit level Information Assurance (IA) Officers. Responsible for cybersecurity risk management of national security systems during all phases of the IS life cycle through Remanence Security (REMSEC). Integrates risk management framework tools with other IS functions to protect and defend IS resources. Advises cyber systems operations personnel and system administrators on known vulnerabilities and assists in developing mitigation and remediation strategies. Provides CIA by verifying cybersecurity controls are implemented in accordance with DoD and Air Force standards. Analyzes risks and/or vulnerabilities and takes corrective action to mitigate or remove them. Ensures appropriate administrative, physical, and technical safeguards are incorporated into all new and existing IS resources through certification and accreditation and protects IS resources from malicious activity. Performs EMSEC duties in accordance with national and DoD EMSEC standards. Denies unauthorized access to classified, and in some instances, unclassified information via compromising emanations within a controlled space through effective countermeasure application. Ensures all systems and devices comply with national and DoD EMSEC standards. Inspects classified work areas, provides guidelines and training, maintains area certifications, determines countermeasures; advises commanders on vulnerabilities, threats, and risks; and recommends practical courses of action. Responsible for oversight or management of installation Information Assurance awareness programs. Performs or supervises user cybersecurity awareness and training. Promotes cybersecurity awareness through periodic training, visual aids, newsletters, or other dissemination methods in accordance with organizational requirements. As part of the Cyberspace Support career field family, manages, supervises, and performs planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as advisor at meetings for facility design, military construction programs and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors status of base work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system installation records, files, and indexes. Evaluates contracts, support, contingency and exercise plans to determine impact on manpower, equipment, and systems.

Special Requirements: Along with the duties specified in this description, this position may augment. Specific areas of responsibility include Information System Security Manager, TEMPEST program manager, project management, COMSEC Responsible Officer (CRO), Secure Voice Responsible Officer (SVRO). The communications section at the CRTC is responsible for providing this support to the CRTC, tenant units, and deployed personnel. Responsible for the vulnerability management program along with proficiency utilizing the tools provided by the AF (ACAS, eMASS, HBSS, etc…) as well as commercial cyber security tools required to meet local needs. Must be knowledgeable in the software certification process, IT portfolio management (ITIPS), DIACAP/RMF processes and procedures required to maintaining existing C&A/A&A for systems and enclaves. The ability to effectively interact with and support communications requirements to a wide variety of customers is imperative. Excellent verbal and written communications skills are required. Implements and interprets policies, directives and procedures. Evaluates effectiveness of equipment usage, systems performance, customer service, supplies, and system scheduling, processing, and maintenance. This position requires a broad experience base and flexibility to meet the need as it arises, and requires an individual who continues to improve their skills outside of the Monday through Friday workday. It is a high demand position, but is also rewarding for someone with a true passion for the career field as you will have the opportunity to work in many aspect of the 3DXXX field.

SPECIALTY QUALIFICATIONS:

Knowledge. Knowledge is mandatory of: IS resources; capabilities, functions and technical methods for IS operations; organization and functions of networked IS resources; communications-computer flows, operations and logic of electromechanical and electronics
IS and their components, techniques for solving IS operations problems; and IS resources security procedures and programs including
Internet Protocols.

Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory.
Additional courses or certifications in computer and information systems technology are desirable. Any network or computing
commercial certification is desirable. DoD 8570.01-M IAM level II certification is mandatory at a minimum and continued training along the IAT level II and IAM Level II tracks are required (Microsoft, Avaya, ISC2, SANS, ISA, etc…).

Training. For award of AFSC 3D033, completion of Cyber Surety initial skills course is mandatory.

Experience. The following experience is mandatory for award of the AFSC indicated:
3.4.1. 3D053. Qualification in and possession of AFSC 3D033. Experience performing cybersecurity functions and/or activities.
3.4.2. 3D073. Qualification and possession of AFSC 3D053. Experience supervising cybersecurity functions and/or activities or
resource and project management.

Other. The following are mandatory as indicated:

3.5.1. For entry into this specialty, see attachment 4 for entry requirements.
3.5.2. For award and retention of this AFSC, individual must maintain local network access IAW AFMANs 17-1201, *User Responsibilities and Guidance for Information Systems* and 17-1301, *Computer Security.*
3.5.2.1. Specialty routinely requires work in the networking environment.
3.5.2.2. Must attain and maintain a minimum Information Assurance Management Level II certification according to DoD 8570.01-M, *Information Assurance Workforce Improvement Program*.
3.5.2.3. Specialty requires routine access to Top Secret material or similar environment.
3.5.2.4. Completion of a current Single Scope Background Investigation (SSBI) according to AFI 31-501, *Personnel Security Program Management,* is mandatory.
NOTE: Award of the 3-skill level without a completed SSBI is authorized provided an interim Top Secret security clearance has been granted according to AFI 31-501.

HOW TO APPLY

All applicants must submit a complete application packet to J1 to be considered for an AGR position. All Applicants must submit an application that includes the following:

- ☐ Cover letter with Job Announcement Number and Position Title for which you are applying, current Military Status (AGR, Technician, Traditional, Active Duty), along with contact information (i.e. Phone numbers and an e-mail address). **Required for all applications.**

- ☐ If you are unable to obtain or must substitute required documents, a detailed statement must be provided in the Application Cover letter to justify the absence. **Failure to include justification for missing or replaced documentation in cover letter will result in disqualification of Application. Documents submitted after the closing date will not be accepted.**

- ☐ NGB Form 34-1 (Application for AGR Position) dated 11 November 2013 **(must be provided even if already AGR; must be signed and dated).** Manually signed copy accepted. Digital signature may fall off when combining PDF files. Double check prior to sending packet.

- ☐ Record Review RIP (**NOT point credit summary or Career Data Brief**) complete and current. Other Service Components submit appropriate individual personnel information printout. This is used to verify AFSCs, aptitude scores, position status, time in service, time in grade, etc. This can be pulled from VMPF. If you cannot pull contact your A1.

- ☐ All airmen will provide a satisfactory fitness test by the last day of the month, not outside 12 calendar months (must meet this requirement by the closing date).

- ☐ Current (within 12 months) **AF Form 422**, Physical Profile Serial Report. Other Service Components submit medical documentation that includes PULHES score and if any PULHES are a "3", a statement indicating that individual is Worldwide Deployable. If you do not know where to obtain a 422 contact your Medic section. A working copy will be accepted to show the process has been started if most current 422 is not within 12 months of the closing date. This is used to verify PULHES and medical readiness.

- ☐ DMA FORM 181-E (Race and National Origin Identification) dated OCT 2006.*

  **The Wisconsin National Guard is an organization that values diversity and inclusion. As part of our recruitment process, we invite all job seekers interested in employment with The Wisconsin National Guard to voluntarily provide gender and ethnic information for *Equal Employment Opportunity reporting. We do not use this self-identification information in any manner to make our hiring decisions, and whether or not you provide your self-identification information will have no impact on our review of your resume and/or application.*

- ☐ All Other Service Component applicants must have their **ASVAB** raw scores converted to Air Force ASVAB scores and include them in a letter from either a Recruiter or MEPS Counselor.

1. E-mail **SCANNED** application encrypted to AGR POCs SSG Jennifer Valencia and SSgt Ryan Olson: jennifer.r.valencia2.mil@mail.mil and ryan.e.olson9.mil@mail.mil An email will be sent to confirm receipt of application. **Emails verifying receipt are not automatic**. Feel free to call Comm (608) 242-3720 or (608) 242-3730 to verify receipt of your packet. Scan file in as 1 PDF. Contact your unit to assist if needed.

2. Applications can also be mailed at applicant's own expense (next day mail suggested) or hand carried to: Joint Force Headquarters Wisconsin, ATTN: **WIJS-J1-AGR (AGR Army Staffing)**, 2400 Wright Street, Madison, WI 53704-2572. Do not submit application packets in three-ring binders, 2 sided, on card stock, or staple pages together. Must be received prior to closing date or it will be disqualified (do not mail out the last day job announcement is open!) Individuals may call 608-242-3720 or 608-242-3730 before job-closing date to ensure the application was received.

3. **J1 will not review the application for completion or accuracy before the closing date. The applicant is responsible to ensure that application is complete and all required documents are correct and included.** If the application is incomplete, a letter will be sent to the individual indicating the reason for disqualification. All applications submitted become the property of the Human Resources Office and will not be returned.

4. Questions regarding this announcement may be referred to AGR Army Staffing, Comm (608) 242-3718 DSN 724-3718 or e-mail Ng.wi.wiarng.mbx.j1-internet-feedback@mail.mil